PN - DE10203926 A1 20030814
OPD - 2002-01-31
PA - BRANDT RICHARD [DE]; ZISCHKA GERHARD [DE]
IN - BRANDT RICHARD [DE]; NICKLAS ANDREAS [DE]; ZISCHKA GERHARD [DE]
TI - Data carrier e.g. smart card with personal data security, has storage element for encoded person-specific data based on biometric characteristics
AB - Data carrier (10) has at least one storage element. On the storage element encoded, person-specific data (2), based on the biometric characteristics of at least one card user, is stored. Biometric characteristics are fingerprints for several fingers of authorized user, voice recordings or anatomical data. Sensor (1) on card detects current user's biometric characteristics to be compared with data stored on the card.
EC - G06F21/00N5A2B; G06F21/00N5A2D; G06K19/073A4A; G06K19/077; G07C9/00B6D4; G11B20/00P
ECI - G06K19/077; G11B20/00P
IC - G06K19/06; G06K9/62
ICAI - G06F21/00; G06K19/073; G06K19/077; G07C9/00; G11B20/00
ICCI - G06F21/00; G06K19/073; G06K19/077; G07C9/00; G11B20/00
AP - DE20021003926 20020131
PR - DE20021003926 20020131
FAMN - 27588198
PD - 2003-08-14
TXT - biometrics

AN - 2003-681194 [65]
OPD - 2002-01-31
PD - 2003-08-14
AP - DE20021003926 20020131
PA - (BRAN-I) BRANDT R
- (ZISC-I) ZISCHKA G
CPY - BRAN-I; ZISC-I
IN - BRANDT R; NICKLAS A; ZISCHKA G
TI - Data carrier e.g. smart card with personal data security, has storage element for encoded person-specific data based on biometric characteristics
AB - NOVELTY :
Data carrier (10) has at least one storage element. On the storage element encoded, person-specific data (2), based on the biometric characteristics of at least one card user, is stored. Biometric characteristics are fingerprints for several fingers of authorized user, voice recordings or anatomical data. Sensor (1) on card detects current user's biometric characteristics to be compared with data stored on the card.
- USE :
As smart cards with security check to check that card user is authorized card user.
- ADVANTAGE :
The legitimate person can be identified with a high degree of reliability as prints of several fingers of user can be stored, or several voice recordings etc., can be used by one or several authorized users.
- DESCRIPTION OF DRAWINGS :
A schematic representation of the data carrier is shown.
1 : Sensor
2 : Electronic finger print
3 : Data processing program
4 : Processor
5 : Read/write device
10 : Smart card
20 : External authority
PN - DE10203926 A1 20030814 DW200365

NC - 1
IW - DATA CARRY SMART CARD PERSON SECURE STORAGE ELEMENT ENCODE SPECIFIC BASED CHARACTERISTIC
IC - G06K19/06; G06K9/62
MC - S05-D01C5A T04-D04 T04-D07 T05-L03C5
DC - S05 T04 T05

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 03 926 A 1**

(51) Int. Cl.[7]:
G 06 K 19/06
G 06 K 9/62

(21) Aktenzeichen: 102 03 926.7
(22) Anmeldetag: 31. 1. 2002
(43) Offenlegungstag: 14. 8. 2003

(71) Anmelder:
Brandt, Richard, 82041 Oberhaching, DE; Zischka, Gerhard, 85354 Freising, DE

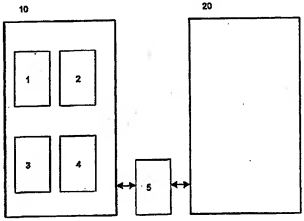
(72) Erfinder:
Brandt, Richard, 82041 Oberhaching, DE; Nicklas, Andreas, 82041 Oberhaching, DE; Zischka, Gerhard, 85354 Freising, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Datenträger mit mindestens einem Speicherelement

(57) Die Aufgabe, einen Datenträger bereitzustellen, der so beschaffen ist, daß eine berechtigte Person mit hoher Zuverlässigkeit identifiziert werden kann, wird durch den erfindungsgemäßen Datenträger mit mindestens einem Speicherelement gelöst, wobei auf dem Speicherelement mindestens verschlüsselte, personenspezifische Daten für eine unbestimmte Zeitdauer gespeichert sind, die auf biometrische Charakteristiken mindestens einer Person beruhen und die zur Personalisierung zumindest dieser einen Person dienen.



DE 102 03 926 A 1

DE 102 03 926 A 1

Beschreibung

[0001] Die Erfindung richtet sich auf einen Datenträger mit mindestens einem Speicherelement.

[0002] Im Stand der Technik sind Datenträger, insbesondere Chipkarten bekannt, die zur Identifizierung des Benutzers bzw. als Berechtigungsnachweis zur Benutzung sogenannte PIN's (persönliche Identifikationsnummern) oder Passwörter verwenden.

[0003] Chipkarten haben den Nachteil, daß nicht festgestellt werden kann, ob der Benutzer der Chipkarte auch der berechtigte Eigentümer ist. Einerseits kann die Chipkarte gestohlen werden, andererseits kann die PIN oder das Passwort ausgespäht oder gestohlen werden, so daß unberechtigte Personen die Chipkarte benutzen können.

[0004] Aufgabe der vorliegenden Erfindung ist es daher, einen Datenträger bereitzustellen, der so beschaffen ist, daß die berechtigte Person mit hoher Zuverlässigkeit identifiziert werden kann.

[0005] Diese Aufgabe wird durch den erfindungsgemäßen Datenträger mit den Merkmalen gemäß Anspruchs 1 gelöst. Vorteilhafte Weiterbildungen der vorliegenden Erfindung sind in den Unteransprüchen gekennzeichnet.

[0006] Der erfindungsgemäße Datenträger weist mindestens ein Speicherelement auf, wobei auf dem Speicherelement mindestens verschlüsselte, personenspezifische Daten, die auf biometrische Charakteristiken mindestens einer Person beruhen und die zur Personalisierung zumindest dieser einen Person dienen für eine unbestimmte Zeitdauer gespeichert sind.

[0007] Vorteilhafterweise sind diese biometrischen Charakteristiken Fingerabdrücke und/oder Stimmabdrücke und/oder andere Daten, wie beispielsweise anatomische Maße (z. B. Gesichtskonturen, Knochengeometrien), Irisbeschaffenheit, o. ä.

[0008] Vorteilhafterweise sind auf dem erfindungsgemäßen Datenträger mehrere verschlüsselte, personenspezifische Datensätze einer Person, insbesondere Datensätze von mehreren Personen gespeichert.

[0009] Zweckmäßigerweise ist auf dem Datenträger ein Sensor angeordnet, der so ausgebildet ist, daß die biometrischen Charakteristiken erfaßbar sind. Bei einer anderen Ausführungsform des erfindungsgemäßen Datenträgers, weist dieser weiterhin einem Prozessor auf, der so ausgebildet ist, ein Vergleichsverfahren zwischen einer personenspezifischen Datenmenge, die nicht auf dem Datenträger gespeichert ist mit einer Datenmenge, die auf dem Datenträger gespeichert ist vorzunehmen und ein Vergleichsergebnis zu ermitteln.

[0010] Zur Übertragung dieses Vergleichsergebnis weist eine weitere Ausführungsform des erfindungsgemäßen Datenträgers ein Mittel auf, das so ausgebildet ist, das Vergleichsergebnis zu einer externen Einheit zu übertragen.

[0011] Nachfolgend ist die Erfindung an einem Ausführungsbeispiel näher erläutert, wobei der Datenträger als Chipkarte und die biometrischen Daten als Fingerabdrücke ausgebildet sind.

[0012] Der erfindungsgemäße Datenträger weist unter anderem den Vorteil auf, daß bspw. nicht nur ein Fingerabdruck sondern mehrere Fingerabdrücke auf einer Chipkarte abgespeichert werden können.

[0013] Nach dem Abspeichern mehrerer Fingerabdrücke auf einer Chipkarte kann die Fehlerrate des falschen Abweisens durch redundantes Überprüfen wesentlich reduziert werden. Ebenso kann die Sicherheit der Authentifizierung eines Benutzers der Chipkarte auf der Basis mehrerer Fingerabdrücken durch mehrfaches Überprüfen erhöht werden. Fingerabdrücke die auf unterschiedlichen Worten basieren

ermöglichen zudem einen zufallgesteuerten Dialog, der die Sicherheit der Authentifizierung zusätzlich erhöht.

[0014] Die Chipkarte kann auf Basis von Fingerabdrücken nicht nur einer Person, sondern auch einer Gruppe von Personen zugeordnet werden. Dies wird erreicht, indem die elektronischen Fingerabdrücke unterschiedlicher Personen auf der gleichen Chipkarte abgespeichert werden. Die Chipkarte kann einer Gruppe von Menschen eindeutig zugeordnet werden, so daß ausschließlich die Personen, die dieser Gruppe angehören, eine Berechtigungsanfrage positiv beantwortet erhalten.

[0015] Zum Abspeichern der verschlüsselten, biometrischen Daten werden beispielsweise die Stimm- oder Fingerabdrücke über eine Aufnahmeeinrichtung (Mikrofon, Recorder) oder Scannen erfaßt und mit einem geeigneten Verfahren in einen binären Datensatz umgewandelt. Dieser bestimmte Datensatz wird auf der Chipkarte gespeichert. Zweckmäßigerweise wird mit dem Umwandlungsverfahren ein bestimmter Datensatz erzeugt, der nicht mehr in ein entsprechendes biometrisches Muster (bspw. Stimm- oder Fingerabdruck) rückumgewandelt werden kann.

[0016] Vorteilhafterweise ist das Umwandlungsverfahren als Programm auf der erfindungsgemäßen Chipkarte gespeichert. Ebenso kann der Sensor zur Erfassung der biometrischen Charakteristika auf dem erfindungsgemäßen Datenträger angeordnet sein. Erfindungsgemäß ist es aber auch möglich, den Sensor auf einem externen Gerät anzuordnen und die biometrischen Charakteristika sowohl in umgewandelte als auch nicht umgewandelter Form mit Hilfe eines Lese- und Schreibgerätes auf den Datenträger, beispielsweise der Chipkarte abzuspeichern.

[0017] Nachfolgend ist ein Verfahren zur Authentifizierung eines Benutzers einer Chipkarte mit einem elektronischen Fingerabdruck näher erläutert, wie es beispielsweise bei dem erfindungsgemäßen Datenträger angewandt wird.

[0018] Wenn eine Person oder eine Gruppe von Personen eine Chipkarte mit elektronischen Fingerabdruck benutzt, so werden diese zweckmäßigerweise bei jeder Benutzung der Chipkarte authentifiziert.

[0019] Die Authentifizierung erfolgt durch den aktuellen Vergleich der mittels eines Sensors erfassten Fingerabdrucks mit dem oder den auf der Chipkarte abgelegten Fingerabdrücken. Der Vergleich kann in einem engen Zeitfenster von wenigen Sekunden erfolgen, damit ein echtzeitfähiger Vergleich einen Missbrauch verhindern kann. Der Vergleich des aktuell erfassten Fingerabdrucks mit dem auf der Chipkarte abgespeicherten elektronischen Fingerabdrucks erfolgt zweckmäßigerweise mit einem Datenverarbeitungsprogramm.

[0020] Dieses Datenverarbeitungsprogramm zur Verifikation des Fingerabdrucks kann sich sowohl auf der Chipkarte als auch auf einem externen Rechner befinden. Die Ausführung des Datenverarbeitungsprogramms zur Authentifizierung eines Benutzers einer Chipkarte kann entweder auf der Chipkarte selbst oder auf einem externen Rechner erfolgen.

[0021] Aufgrund der mit dem Fingerabdruck gemeinsam auf der Chipkarte gespeicherten Daten, wie zum Beispiel dem Namen einer Person, erfolgt eine eindeutige Identifizierung einer Person.

[0022] Sind die Fingerabdrücke einer Gruppe von Personen auf einer Chipkarte abgespeichert, so liefert das Datenverabeitungsprogramm als Ergebnis nicht nur die erfolgreiche Verifikation einer Person, sondern auch die zu dem jeweiligen Fingerabdruck gehörigen Daten wie beispielsweise dem Namen.

[0023] Ebenso unterstützt die Erfindung, daß zwei oder mehrere verschiedene Personen authentifiziert werden müssen, bevor die mit der Chipkarte verbundene Berechtigungs-

anfrage positiv beantwortet wird.

[0024] Hierbei werden die Personen auf Basis der auf der Chipkarte abgespeicherten Fingerabdrücken nacheinander oder parallel authentifiziert. Erst bei der erfolgreichen Authentifizierung mehrerer Personen ermöglicht das Datenverarbeitungsprogramm beispielsweise die Benutzung der Chipkarte.

[0025] Nachfolgend sind 4 Ausführungsbeispiele der vorliegenden Erfindung anhand von Figuren näher erläutert. Es zeigen:

[0026] **Fig. 1** eine schematische Darstellung einer erste Ausführungsform der vorliegenden Erfindung;

[0027] **Fig. 2** eine schematische Darstellung einer zweiten Ausführungsform der vorliegenden Erfindung;

[0028] **Fig. 3** eine schematische Darstellung einer vierten Ausführungsform der vorliegenden Erfindung;

[0029] **Fig. 4** eine schematische Darstellung einer fünften Ausführungsform der vorliegenden Erfindung.

[0030] In **Fig. 1** ist ein Sensor **1** gezeigt, der auf einer Chipkarte **10** angeordnet ist und der Erfassung von biometrischen Charakteristika, beispielsweise Fingerabdrücken dient. Die Fingerabdrücke werden mittels Datenverarbeitungsprogramm **3**, welches sich ebenfalls auf der Chipkarte **10** befindet als elektronische Fingerabdrücke **2** in verschlüsselter Form abgespeichert bzw. verifiziert und identifiziert. Das Datenverarbeitungsprogramm **3** wird auf dem Prozessor **4** ausgeführt, der ebenfalls auf der Chipkarte **10** angeordnet ist. Das Ergebnis einer positiven oder negativen Authentifizierung, sowie die Identifikationsdaten werden an externe Instanzen **20**, bspw. mittels eines Chipkarten Lese-/Schreibgerätes **5** übermittelt.

[0031] Gemäß einer zweiten Ausführungsform, dargestellt in **Fig. 2** dient der externe Sensor **1** zur Erfassung von Fingerabdrücken. Die Fingerabdrücke werden mittels Datenverarbeitungsprogramm **3**, die sich auf der Chipkarte **10** befindet als elektronische Fingerabdrücke **2** auf der Chipkarte **10** in verschlüsselter Form abgespeichert bzw. verifiziert und identifiziert. Das Datenverarbeitungsprogramm **3** wird auf dem Prozessor **4** ausgeführt. Das Ergebnis einer positiven oder negativen Authentifizierung, sowie die Identifikationsdaten werden an externe Instanzen **20**, bspw. mittels eines Chipkarten Lese-/Schreibgerätes **5** übermittelt.

[0032] In einer weiteren Ausführungsform der vorliegenden Erfindung wird gemäß **Fig. 3** ein externer Sensor **1** zur Erfassung von Fingerabdrücken verwendet. Der Fingerabdruck wird mittels Datenverarbeitungsprogramm **3**, das sich auf der Chipkarte **10** befindet als elektronische Fingerabdrücke **2** auf der Chipkarte **10** in verschlüsselter Form abgespeichert bzw. verifiziert und identifiziert. Das Datenverarbeitungsprogramm **3** wird auf dem externen Prozessor **4** ausgeführt. Das Ergebnis einer positiven oder negativen Authentifizierung, sowie die Identifikationsdaten werden an externe Instanzen **20**, bspw. mittels eines Chipkarten Lese-/Schreibgerätes **5** übermittelt.

[0033] In einer weiteren erfindungsgemäßen Ausführungsform, dargestellt in **Fig. 4**, wird der externe Sensor **1** zur Erfassung von Fingerabdrücken verwendet, wobei die Fingerabdrücke mittels Datenverarbeitungsprogramm **3** als elektronische Fingerabdrücke **2** auf der Chipkarte **10** in verschlüsselter Form abgespeichert werden. Das Datenverarbeitungsprogramm zum Erfassen, Verschlüsseln, Verifizieren und Identifizieren der Fingerabdrücke wird auf dem externen Prozessor **4** ausgeführt. Das Ergebnis einer positiven oder negativen Authentifizierung, sowie die Identifikationsdaten werden an externe Instanzen **20**, bspw. mittels eines Chipkarten Lese-/Schreibgerätes **5** übermittelt.

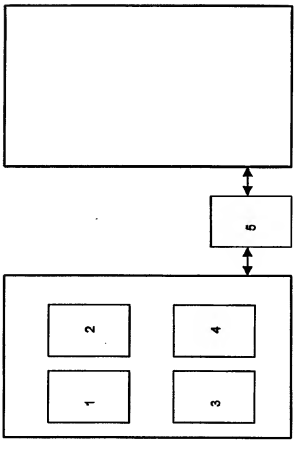
Patentansprüche

1. Datenträger (**10**) mit mindestens einem Speicherelement, wobei auf dem Speicherelement zumindest verschlüsselte, personenspezifische Daten (**2**), die auf biometrische Charakteristiken mindestens einer Person beruhen und die zur Personalisierung zumindest dieser einen Person dienen für eine unbestimmte Zeitdauer gespeichert sind.
2. Datenträger (**10**) nach Anspruchs 1, wobei die biometrischen Charakteristiken Fingerabdrücke und/oder Stimmabdrücke sind.
3. Datenträger (**10**) nach Anspruch 1 oder 2, wobei mehrere verschlüsselte, personenspezifische Daten (**2**) einer Person gespeichert sind.
4. Datenträger (**10**) nach einem der vorherigen Ansprüche, wobei mehrere verschlüsselte Daten (**2**) von mehreren Personen gespeichert sind.
5. Datenträger (**10**) nach einem der vorherigen Ansprüche, weiterhin bestehend aus einem Sensor, der so ausgebildet ist, daß die biometrischen Charakteristiken erfaßbar sind.
6. Datenträger (**10**) nach einem der vorherigen Ansprüche, weiterhin bestehend aus einem Prozessor (**4**), der so ausgebildet ist, ein Vergleichsverfahren zwischen einem personenspezifischen Datenmenge, die nicht auf dem Datenträger gespeichert ist mit einer Datenmenge, die auf dem Datenträger gespeichert vorzunehmen und ein Vergleichsergebnis zu ermitteln.
7. Datenträger (**10**) nach Anspruch 6, weiterhin bestehend aus einem Mittel, daß so ausgebildet ist, das Vergleichsergebnis zu einer externen Einheit zu übertragen.

Hierzu 4 Seite(n) Zeichnungen

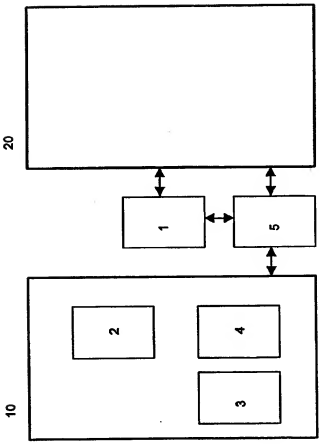
- Leerseite -

Nummer: DE 102 03 926 A1
Int. Cl.[7]: G 06 K 19/06
Offenlegungstag: 14. August 2003



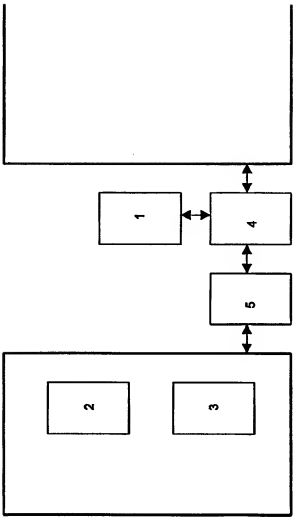
Figur 1

Nummer: DE 102 03 926 A1
Int. Cl.[7]: G 06 K 19/06
Offenlegungstag: 14. August 2003



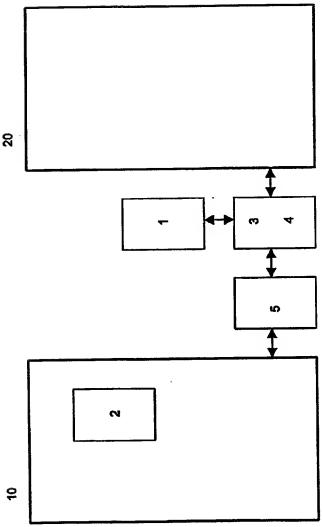
Figur 2

Nummer: DE 102 03 926 A1
Int. Cl.[7]: G 06 K 19/06
Offenlegungstag: 14. August 2003



Figur 3

Nummer: DE 102 03 926 A1
Int. Cl.[7]: G 06 K 19/06
Offenlegungstag: 14. August 2003



Figur 4